WHAT IS CLAIMED IS:

1. An exponent calculation apparatus for calculating x^e based on two integers x and e, the apparatus comprising:

an input unit for inputting the two integers x and e;

a candidate exponents storing unit for storing candidate exponents {l_i} (0≤i≤L-1), the number of the candidate exponents being L;

a pre-calculation unit for pre-calculating x^{l_i} for each of the candidate exponents {l_i}, which are stored in the candidate exponents storing unit, based on the input integer x;

a pre-calculated values storing unit for storing the values x^{l_i} obtained by the pre-calculation;

a dividing unit for dividing the input integer e into a plurality of values {f_i} (0≤i≤F-1) so that each of the values {f_i} corresponds to one of the candidate exponents {l_i};

a calculation result storing unit for storing a calculation result c;

a sequential processing unit for sequentially updating the calculation result c for each of the divided values {f_i} (0≤i≤F-1) by using each of the pre-calculated values x^{l_i}; and

an output unit for outputting the updated calculation result c for each of the values {f_i} as x^e.

2. An exponent calculation apparatus for calculating x^e(mod N) based on three integers x, e, and N, the apparatus comprising:

an input unit for inputting the three integers x, e, and N;

a candidate exponents storing unit for storing candidate exponents {l_i} (0≤i≤L-1), the number of the candidate exponents being L;

a pre-calculation unit for pre-calculating x^{l_i} for each of the candidate exponents {l_i}, which are stored in the candidate exponents storing unit, based on the input integer x;

a pre-calculated values storing unit for storing the values x^{l_i} obtained by the pre-calculation;

a dividing unit for dividing the input integer e into a plurality of values {f_i} (0≤i≤F-1) so that each of the values {f_i} corresponds to one of the candidate exponents {l_i};

a calculation result storing unit for storing a calculation result c;

a sequential processing unit for sequentially updating the calculation result c for each of the divided values {f_i} (0≤i≤F-1) by using each of the pre-calculated values x^{l_i}; and

an output unit for outputting the updated calculation result c for each of the values {f_i} as x^e(mod N).

3. The apparatus according to Claim 2, wherein the sequential processing unit comprises:

an initializing unit for setting f_0, which is an initial value of the calculation result c, in the calculation result storing unit; and

an updating unit for updating bit length represented by $c:=c^2$ of each of the divided values {f_i} (0≤i≤F-1) in binary notation and updating c:=c*f_i.

4. The apparatus according to Claim 2, wherein the candidate exponents stored in the candidate exponents storing unit have a form of (0) or 1$[01]_L$ in binary notation, where $[xy]_i$ means that xy is repeated i times.

5. The apparatus according to Claim 2, wherein the candidate exponents stored in the candidate exponents storing unit have a form of (0), (11), or 1$[01]_L$ in binary notation, where $[xy]_i$ means that xy is repeated i times.

6. The apparatus according to Claim 2, wherein the dividing unit divides (10) in a bit string of the divided

values represented in binary notation into (01) and (01) so that the values {f_i} may be overlapped, and, in an updating process of $c:=c^2$ by the sequential processing unit, an overlapped portion of bit length of the values f_i is not updated.

7. The apparatus according to Claim 2, further comprising:

a multiplication number estimating unit for estimating the number of multiplications according to division performed by the dividing unit; and

a division controlling unit for controlling division performed by the dividing unit based on the estimated number of multiplications.

8. The apparatus according to Claim 7, wherein the multiplication number estimating unit estimates the number of multiplications by assigning different weights to multiplication of different values and multiplication of same values.

9. The apparatus according to Claim 2, wherein the number L of the candidate exponents, which are stored in the candidate exponents storing unit, is increased or decreased depending on the bit length of the input value e.

10. The apparatus according to Claim 2, wherein each of the candidate exponents stored in the candidate exponents storing unit is 0 or a binary number of W bits or less, and has a form $1[01]_L$, $11[01]_L$, or $1[01]_L1$, where $[xy]_i$ means that xy is repeated i times.

11. The apparatus according to Claim 10,

wherein the pre-calculation unit uses four functions $f_1()$, $f_2()$, $f_3()$, and $f_4()$, which represent the candidate exponents,

sets initial values: $f_1(0)=1$, $f_2(0)=0$, $f_3(0)=1$, and $f_4(0)=1$,

performs circular calculation so as to satisfy $f_1(i)=f_2(i-1)+f_4(i-1)$, $f_2(i)=f_1(i)+f_3(i-1)$, $f_3(i)=f_2(i)+f_3(i-1)$, and $f_4(i)=f_1(i)+f_2(i)$ and obtains forms $f_1(i)=1[01]_i$, $f_2(i)=10[00]_i$, $f_3(i)=11[01]_i$, and $f_4(i)=1[01]_i1$ so as to form an addition chain,

calculates $x^{f1(i)}$ based on the product of $x^{f2(i-1)}$ and $x^{f4(i-1)}$, $x^{f2(i)}$ based on the product of $x^{f1(i)}$ and $x^{f3(i-1)}$, $x^{f3(i)}$ based on the product of $x^{f2(i)}$ and $x^{f3(i-1)}$, and $x^{f4(i)}$ based on the product of $x^{f1(i)}$ and $x^{f2(i)}$, and

stores the calculation result in the calculation result storing unit.

12. The apparatus according to Claim 10,

wherein the calculation result storing unit includes four array regions $F_1()$, $F_2()$, $F_3()$, and $F_4()$ for storing calculation results and sets initial values $F_1(0)=x$, $F_2(0)=1$, $F_3(0)=x$, and $F_4(0)=x$, and

the pre-calculation unit performs circular calculation so as to satisfy $F_1(i)=F_2(i-1)*F_4(i-1)$, $F_2(i)=F_1(i)*F_3(i-1)$, $F_3(i)=F_2(i)*F_3(i-1)$, and $F_4(i)=F_1(i)*F_2(i)$ and stores the calculation result in the calculation result storing unit.

13. The apparatus according to Claim 10, wherein the bit number W of each of the candidate exponents stored in the candidate exponents storing unit is changed in accordance with the bit number of the integer e.

14. An exponent calculation method for calculating x^e based on two integers x and e, the method comprising:

an input step of inputting the two integers x and e;

a pre-calculation step of pre-calculating x^{l_i} for each of candidate exponents {l_i} (0≤i≤L-1) stored in a candidate exponents storing unit, the number of the candidate exponents being L, based on the input integer x, and storing the values x^{l_i} obtained by the pre-calculation in a pre-calculated values storing unit;

a dividing step of dividing the input integer e into a plurality of values {f_i} (0≤i≤F-1) so that each of the values {f_i} corresponds to one of the candidate exponents {l_i};

a sequential processing step of sequentially updating a calculation result c, which is stored in a calculation result storing unit, for each of the divided values {f_i} (0≤i≤F-1) by using each of the pre-calculated values x^{l_i}; and

an output step of outputting the updated calculation result c for each of the values {f_i} as x^e.

15. An exponent calculation method for calculating x^e(mod N) based on three integers x, e, and N, the method comprising:

an input step of inputting the three integers x, e, and N;

a pre-calculation step of pre-calculating x^{l_i} for each of candidate exponents {l_i} (0≤i≤L-1) stored in a candidate exponents storing unit, the number of the candidate exponents being L, based on the input integer x, and storing the values x^{l_i} obtained by the pre-calculation in a pre-calculated values storing unit;

a dividing step of dividing the input integer e into a plurality of values {f_i} (0≤i≤F-1) so that each of the values {f_i} corresponds to one of the candidate exponents {l_i};

a sequential processing step of sequentially updating a calculation result c, which is stored in a calculation result storing unit, for each of the divided values {f_i} (0≤i≤F-1) by using each of the pre-calculated values x^{l_i}; and

an output step of outputting the updated calculation result c for each of the values {f_i} as x^e(mod N).

16. A computer-readable program for allowing a computer to execute exponent calculation for calculating x^e based on two integers x and e, said program comprising codes for causing the computer to perform:

an input step of inputting the two integers x and e;

a pre-calculation step of pre-calculating x^{l_i} for each of candidate exponents {l_i} (0≤i≤L-1) stored in a candidate exponents storing unit, the number of the candidate exponents being L, based on the input integer x, and storing the values x^{l_i} obtained by the pre-calculation in a pre-calculated values storing unit;

a dividing step of dividing the input integer e into a plurality of values {f_i} (0≤i≤F-1) so that each of the values {f_i} corresponds to one of the candidate exponents {l_i};

a sequential processing step of sequentially updating a calculation result c, which is stored in a calculation result storing unit, for each of the divided values {f_i} (0≤i≤F-1) by using each of the pre-calculated values x^{l_i}; and

an output step of outputting the updated calculation result c for each of the values {f_i} as x^e.

17. A computer-readable program for allowing a computer to execute exponent calculation for calculating x^e(mod N) based on three integers x, e, and N, said program comprising codes for causing the computer to perform:

an input step of inputting the three integers x, e, and N;

a pre-calculation step of pre-calculating x^{l_i} for each of candidate exponents {l_i} (0≤i≤L-1) stored in a candidate exponents storing unit, the number of the candidate exponents being L, based on the input integer x, and storing the values x^{l_i} obtained by the pre-calculation in a pre-calculated values storing unit;

a dividing step of dividing the input integer e into a plurality of values {f_i} (0≤i≤F-1) so that each of the values {f_i} corresponds to one of the candidate exponents {l_i};

a sequential processing step of sequentially updating a calculation result c, which is stored in a calculation result storing unit, for each of the divided values {f_i} (0≤i≤F-1) by using each of the pre-calculated values x^{l_i}; and

an output step of outputting the updated calculation result c for each of the values {f_i} as x^e(mod N).